Computer Forensics

US-CERT

Overview

This paper will discuss the need for computer forensics to be practiced in an effective and legal way, outline basic technical issues, and point to references for further reading. It promotes the idea that the competent practice of computer forensics and awareness of applicable laws is essential for today's networked organizations.

This subject is important for managers who need to understand how computer forensics fits as a strategic element in overall organizational computer security. Network administrators and other computer security staff need to understand issues associated with computer forensics. Those who work in corporate governance, legal departments, or IT should find an overview of computer forensics in an organizational context useful.

What is Computer Forensics?

If you manage or administer information systems and networks, you should understand computer forensics. Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. (The word *forensics* means "to bring to the court.") Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive.

Because computer forensics is a new discipline, there is little standardization and consistency across the courts and industry. As a result, it is not yet recognized as a formal "scientific" discipline. *We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.*

Why is Computer Forensics Important?

Adding the ability to practice sound computer forensics will help you ensure the overall integrity and survivability of your network infrastructure. You can help your organization if you consider computer forensics as a new basic element in what is known as a "defense-in-depth"[1] approach to network and computer security. For instance, understanding the legal and technical aspects of computer forensics will help you capture vital information if your network is compromised and will help you prosecute the case if the intruder is caught.

[1] "Defense in depth is designed on the principle that multiple layers of different types of protection from different vendors provide substantially better protection" <http://netsecurity.about.com/cs/generalsecurity/a/aa112103.htm>.

What happens if you ignore computer forensics or practice it badly? You risk destroying vital evidence or having forensic evidence ruled inadmissible in a court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assign liability if certain types of data are not adequately protected. Recent legislation makes it possible to hold organizations liable in civil or criminal court if they fail to protect customer data.[2]

Computer forensics is also important because it can save your organization money. Many managers are allocating a greater portion of their information technology budgets for computer and network security. International Data Corporation (IDC) reported that the market for intrusion-detection and vulnerability-assessment software will reach 1.45 billion dollars in 2006. In increasing numbers, organizations are deploying network security devices such as intrusion detection systems (IDS), firewalls, proxies, and the like, which all report on the security status of networks.

From a technical standpoint, the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

What are some typical aspects of a computer forensics investigation? First, those who investigate computers have to understand the kind of potential evidence they are looking for in order to structure their search.[3] Crimes involving a computer can range across the spectrum of criminal activity, from child pornography to theft of personal data to destruction of intellectual property. Second, the investigator must pick the appropriate tools to use. Files may have been deleted, damaged, or encrypted, and the investigator must be familiar with an array of methods and software to prevent further damage in the recovery process.

Two basic types of data are collected in computer forensics. *Persistent data* is the data that is stored on a local hard drive (or another medium) and is preserved when the computer is turned off. *Volatile data* is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM). Since volatile data is ephemeral, it is essential an investigator knows reliable ways to capture it.

System administrators and security personnel must also have a basic understanding of how routine computer and network administrative tasks can affect both the forensic process (the potential admissibility of evidence at court) and the subsequent ability to recover data that may be critical to the identification and analysis of a security incident.

---

2 Laws such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, California Act 1798, and others hold businesses liable for breaches in the security or integrity of computer networks.

3 For an overview of the types of crimes that involve a computer and how law enforcement aids investigation, see “How the FBI Investigates Computer Crime” at <http://www.cert.org/tech_tips/FBI_investigates_crime.html >.

Legal Aspects of Computer Forensics

Anyone overseeing network security must be aware of the legal implications of forensic activity. Security professionals need to consider their policy decisions and technical actions in the context of existing laws. For instance, you must have authorization before you monitor and collect information related to a computer intrusion. There are also legal ramifications to using security monitoring tools.

Computer forensics is a relatively new discipline to the courts and many of the existing laws used to prosecute computer-related crimes, legal precedents, and practices related to computer forensics are in a state of flux. New court rulings are issued that affect how computer forensics is applied. The best source of information in this area is the United States Department of Justice's Cyber Crime web site.[4] The site lists recent court cases involving computer forensics and computer crime, and it has guides about how to introduce computer evidence in court and what standards apply. The important point for forensics investigators is that evidence must be collected in a way that is legally admissible in a court case.

Increasingly, laws are being passed that require organizations to safeguard the privacy of personal data. It is becoming necessary to prove that your organization is complying with computer security best practices. If there is an incident that affects critical data, for instance, the organization that has added a computer forensics capability to its arsenal will be able to show that it followed a sound security policy and potentially avoid lawsuits or regulatory audits.

There are three areas of law related to computer security that are important to know about. The first is found in the United States Constitution. The Fourth Amendment[5] allows for protection against unreasonable search and seizure, and the Fifth Amendment allows for protection against self-incrimination. Although the amendments were written before there were problems caused by people misusing computers, the principles in them apply to how computer forensics is practiced.

Second, anyone concerned with computer forensics must know how three U.S. Statutory laws[6] affect them:

- Wiretap Act (18 U.S.C. 2510-22)
- Pen Registers and Trap and Trace Devices Statute (18 U.S.C. 3121-27)
- Stored Wired and Electronic Communication Act (18 U.S.C. 2701-120)

[4] http://www.cybercrime.gov

[5] A detailed analysis of issues surrounding the Fourth Amendment can be found on this web site: <http://caselaw.lp.findlaw.com/data/constitution/amendment04/>.

[6] The text of these laws can be found at the U.S. Department of Justice web site <http://www.usdoj.gov/criminal/cybercrime/cclaws.html>.

Violations of any one of these statutes during the practice of computer forensics could constitute a federal felony punishable by a fine and/or imprisonment. It is always advisable to consult your legal counsel if you are in doubt about the implications of any computer forensics action on behalf of your organization.

Third, the U.S. Federal rules of evidence about hearsay, authentication, reliability, and best evidence must be understood. In the U.S. there are two primary areas of legal governance affecting cyber security actions related to the collection of network data: (1) authority to monitor and collect the data and (2) the admissibility of the collection methods. Of the three areas above, the U.S. Constitution and U.S. Statutory Laws primarily govern the collection process, while the Federal Rules of Evidence deal mostly with admissibility.

If system administrators possess the technical skills and ability to preserve critical information related to a suspected security incident in a forensically sound manner and are aware of the legal issues related to forensics, they will be a great asset to their organization. Should an intrusion lead to a court case, the organization with computer forensics capability will be at a distinct advantage. For a more detailed discussion of these and related topics, see the document on which this paper is based, Nolan's *Forensics Guide to Incident Response for Technical Staff*, and other resources listed below.

Online Resources

Center for Democracy and Technology. *Impact of the McCain-Kerrey Bill on Constitutional Privacy Rights.*
http://www.cdt.org/crypto/legis_105/mccain_kerrey/const_impact.html

CERIAS: Digital Forensics Resources.
http://www.cerias.purdue.edu/research/forensics/resources.php?output=printable

Computer Crime and Intellectual Property Section Criminal Division, United States Department of Justice. *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*. http://www.cybercrime.gov/s&smanual2002.htm

Computer Forensics, Cybercrime and Steganography Resources
http://www.forensics.nl/links/

Computer Forensics World.
http://www.computerforensicsworld.com

Computer Professionals for Social Diversity: Computer Crime Directory.
http://www.cpsr.org/cpsr/computer_crime

Cornell University. *Federal Rules of Evidence.*
http://www.law.cornell.edu/rules/fre/overview.html

Craiger, J. Philip. *Computer Forensics Procedures and Methods.*
http://www.ncfs.ucf.edu/craiger.forensics.methods.procedures.final.pdf

Forensics Information from CERT
http://www.cert.org/forensics/

The Forensics Science Portal
http://www.forensics.ca/index.php

Ghosh, Ajoy. *Guidelines for the Management of IT Evidence.*
http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf

Kessler International - Forensic Accounting, Computer Forensics, Corporate Investigation. http://www.investigation.com/praccap/hightech/compforen.htm

National Center for Forensic Science.
http://www.ncfs.ucf.edu/digital_evd.html

Nolan, Richard, et. al. *Forensics Guide to Incident Response for Technical Staff.*
http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf

Robbins, Judd. *An Explanation of Computer Forensics.*
http://www.computerforensics.net/forensics.htm

Sergienko, Greg S. *Self Incrimination and Cryptographic Keys.*
http://law.richmond.edu/jolt/v2i1/sergienko.html#h1

Printed Resources

Casey, Eoghan. *Digital Evidence and Computer Crime (Second Edition).* San Diego, CA: Academic Press, 2000.

Farmer, Dan; Venema, Wietse. *Forensic Discovery*. Addison-Wesley Professional, 2005.

Nelson, Bill. *Guide to Computer Forensics and Investigations*. Boston, MA: Thomson Course Technology, 2004.